AMENDMENTS TO THE CLAIMS

1. (Previously Presented) A tamper-detection-information embedding apparatus for embedding predetermined information for tamper detection in a digital image signal, said apparatus comprising:

a band division portion operable to divide the digital image signal into a plurality of frequency bands;

an authentication data generation portion operable to generate a pseudo-random number series by using predetermined key data, and to generate authentication data from the pseudo-random number series;

a key data embedding portion operable to embed the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands;

an authentication data embedding portion operable to embed the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands; and

a band synthesis portion operable to reconstruct the digital image signal in which the information has been embedded by using the MRA and the MRR to which data embedding processing is subjected.

2. (Previously Presented) The tamper-detection-information embedding apparatus according to claim 1,

wherein a set value T and a set value m are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size,

wherein said authentication data embedding portion embeds the authentication data in each transform coefficient of the MRR by comparing an absolute value of the transform coefficient with the set value T, and if the absolute value is less than the set value T, setting the transform coefficient to the set value +m or –m depending on a bit value of the authentication data to be embedded, and if the absolute value is not less than the set value T, setting the transform coefficient to an even or odd integer nearest to the value q depending on the bit value of the authentication data to be embedded, and

wherein T is a positive integer and m is an integer not more than T.

3. (Previously Presented) A tamper detecting apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal, said tamper detecting apparatus comprising:

a band division portion operable to divide the digital image signal into a plurality of frequency bands;

a key data extraction portion operable to extract key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands;

an authentication data generation portion operable to generate a pseudo-random number series by using the key data, and to generate authentication data from the pseudo-random number series;

an embedded information extraction portion operable to extract embedded information embedded based on the key data by the specific apparatus from transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands; and

a tamper determination portion operable to compare the embedded information with the authentication data for verification and to determine whether the digital image has been tampered with.

4. (Previously Presented) The tamper detecting apparatus according to claim 3, wherein said tamper determination portion comprises:

a block division portion operable to divide the digital image into a plurality of unit blocks each composed of a predetermined number of pixels;

a regional embedded information read portion operable to read, for each of the unit blocks, embedded information embedded in the transform coefficients of the MRR that represents the same spatial region as the unit block, serially from all of the embedded information extracted by said embedded information extraction portion;

a regional authentication data read portion operable to read, for each of the unit blocks, authentication data corresponding in position to the embedded information serially read by said regional embedded information read portion, serially from all of the authentication data generated by said authentication data generation portion; and

a block-tamper determination portion operable to compare the embedded information serially read with the authentication data serially read and to determine, for each of the unit

blocks, whether the digital image has been tampered with.

5. (Previously Presented) The tamper detecting apparatus according to claim 3,

wherein a set value T is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result,

wherein said embedded information extraction portion extracts the embedded information from each transform coefficient of the MRR by comparing an absolute value of the transform coefficient with the set value T, and if the absolute value is less than the set value T, determining whether a value of the transform coefficient is positive or negative and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and if the absolute value is not less than the set value T, determining whether the value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and

wherein T is a positive integer.

6. (Previously Presented) The tamper detecting apparatus according to claim 4,

wherein a set value T is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result,

wherein said embedded information extraction portion extracts the embedded information from each transform coefficient of the MRR by comparing an absolute value of the transform

coefficient with the set value T, and if the absolute value is less than the set value T, determining whether a value of the transform coefficient is positive or negative and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and if the absolute value is not less than the set value T, determining whether the value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and

wherein T is a positive integer.

7. (Previously Presented) A tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal, said method comprising:

dividing the digital image signal into a plurality of frequency bands;

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series;

embedding the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands;

embedding the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands; and

reconstructing the digital image signal in which the information has been embedded by using the MRA and the MRR to which data embedding processing is subjected.

8. (Previously Presented) The tamper-detection-information embedding method according to claim 7,

wherein a set value T and a set value m are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size,

wherein embedding authentication data includes

comparing an absolute value of the transform coefficient with the set value T;

setting the transform coefficient to the set value +m or –m depending on a bit value of the authentication data to be embedded if the absolute value is less than the set value T, and

setting the transform coefficient to an even or odd integer nearest to the value q depending on the bit value of the authentication data to be embedded if the absolute value is not less than the set value T, and

wherein T is a positive integer and m is an integer not more than T.

9. (Previously Presented) A tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal, said method comprising:

dividing the digital image signal into a plurality of frequency bands;

extracting key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands;

generating a pseudo-random number series by using the key data, and generating authentication data from the pseudo-random number series;

extracting embedded information embedded based on the key data by the specific

apparatus from transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands; and

comparing the embedded information with the authentication data for verification and determining whether the digital image has been tampered with.

10. (Previously Presented) The tamper detecting method according to claim 9, further comprising

dividing the digital image into a plurality of unit blocks each composed of a predetermined number of pixels;

reading, for each of the unit blocks, embedded information embedded in the transform coefficients of the MRR that represents the same spatial region as the unit block, serially from all of the embedded information;

reading, for each of the unit blocks, authentication data corresponding in position to the embedded information serially read, serially from all of the authentication data; and

comparing a series of the embedded information serially read with a series of the authentication data serially read and determining, for each of the unit blocks, whether the digital image has been tampered with.

11. (Previously Presented) The tamper detecting method according to claim 9,

wherein a set value T is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result,

wherein said extracting embedded information includes

comparing an absolute value of the transform coefficient with the set value T,

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and

determining whether the value q is even or odd if the absolute value is not less than the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and

wherein T is a positive integer.

12. (Previously Presented) The tamper detecting method according to claim 10,

wherein a set value T is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result,

wherein said extracting embedded information includes

comparing an absolute value of the transform coefficient with the set value T,

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and

determining whether the value q is even or odd if the absolute value is not less than the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and

wherein T is a positive integer.

13. (Previously Presented) A recording medium on which a program having computer device readable instructions to be run on a computer device is recorded for carrying out a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal, the computer device readable instructions including instructions capable of instructing a computer device to perform the method comprising:

dividing the digital image signal into a plurality of frequency bands;

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series;

embedding the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands;

embedding the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands; and

reconstructing the digital image signal in which the information has been embedded by using the MRA and the MRR to which data embedding processing is subjected.

14. (Previously Presented) The recording medium according to claim 13,

wherein a set value T and a set value m are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size,

wherein said embedding authentication data includes:

comparing an absolute value of the transform coefficient with the set value T,

setting the transform coefficient to the set value +m or –m depending on a bit value of the authentication data to be embedded if the absolute value is less than the set value T, and

setting the transform coefficient to an even or odd integer nearest to the value q depending on the bit value of the authentication data to be embedded if the absolute value is not less than the set value T, and

wherein T is a positive integer and m is an integer not more than T.

15. (Previously Presented) A recording medium on which a program having computer device readable instructions to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal, the computer device readable instructions including instructions capable of instructing a computer device to perform the method comprising:

dividing the digital image signal into a plurality of frequency bands;

extracting key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands;

generating a pseudo-random number series by using the key data, and generating authentication data from the pseudo-random number series;

extracting embedded information embedded based on the key data by the specific apparatus from transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands; and

comparing the embedded information with the authentication data for verification and determining whether the digital image has been tampered with.

16. (Previously Presented) The recording medium according to claim 15, wherein the computer device readable instructions include instructions capable of instructing a computer device to perform the method further comprising:

dividing the digital image into a plurality of unit blocks each composed of a predetermined number of pixels;

reading, for each of the unit blocks, embedded information embedded in the transform coefficients of the MRR that represents the same spatial region as the unit block, serially from all of the embedded information;

reading, for each of the unit blocks, authentication data corresponding in position to the embedded information serially read, serially from all of the authentication data; and

comparing a series of the embedded information serially read with a series of the authentication data serially read and determining, for each of the unit blocks, whether the digital image has been tampered with.

17. (Previously Presented) The recording medium according to claim 15,

wherein a set value T is predetermined and q is predetermined as a value obtained by dividing a transform coefficient is divided by a predetermined quantization step size and then rounding off the result,

wherein said extracting embedded information includes

comparing an absolute value of the transform coefficient with the set value T,

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and

determining whether the value q is even or odd if the absolute value is not less than the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and

wherein T is a positive integer.

18. (Previously Presented) The recording medium according to claim 16,

wherein a set value T is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result,

wherein said extracting embedded information includes

comparing an absolute value of the transform coefficient with the set value T,

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and

determining whether the value q is even or odd if the absolute value is not less than the set value T, and extracting a bit value of embedded information embedded in the transform coefficient based on the determination, and

wherein T is a positive integer.

19. (New) A tamper-detection-information embedding apparatus for embedding predetermined information for tamper detection in a digital image signal, said apparatus comprising:

a band division portion operable to divide the digital image signal of an entire image on which no block division is performed into a plurality of frequency bands;

an authentication data generation portion operable to generate a pseudo-random number series by using predetermined key data, and to generate authentication data from the pseudo-random number series;

a key data embedding portion operable to embed the key data in transform coefficients of a lowest frequency band among the plurality of frequency bands;

an authentication data embedding portion operable to embed the authentication data in transform coefficients of the frequency bands exclusive of the lowest frequency band among the plurality of frequency bands; and

a band synthesis portion operable to reconstruct the digital image signal in which the information has been embedded by using the lowest frequency band and the frequency bands exclusive of the lowest band to which data embedding processing is subjected.